Oversight Hearing on
PRIVACY AND CIVIL LIBERTIES IN THE HANDS OF THE GOVERNMENT
POST-SEPTEMBER 11, 2001: RECOMMENDATIONS OF
THE 9/11 COMMISSION AND THE U.S. DEPARTMENT OF DEFENSE
TECHNOLOGY AND PRIVACY ADVISORY COMMITTEE

Committee of the Judiciary
Subcommittee on Commercial and Administrative Law
and Subcommittee on the Constitution
U.S. House of Representatives
August 20, 2004

Prepared Statement of
John O. Marsh, Jr.[*]

Chairmen Chabot and Cannon, Distinguished Members:

I appreciate the opportunity to testify today about the work and final recommendations of the Technology and Privacy Advisory Committee appointed by Secretary of Defense Rumsfeld and chaired by the Honorable Newton N. Minow, one of the nation' most experienced and distinguished public servants. The Committee was created to examine the issues that are the subject of today's hearing—the impact of the government's use of personal information on privacy and civil liberties. Although our charge focused on the Department of Defense, we rapidly discovered that the issues, as well as the data mining activities that raise them, occur throughout the government and require attention.

I applaud your leadership and that of your colleagues on the Committee in holding today's hearing. As a former Member of Congress and Secretary of the Army, I know that few issues could be more important than the security of the Republic or the civil liberties of its citizens. Ensuring that both are rigorously protected is a critical obligation of all branches of Government—but especially of the Congress—and I congratulate you for embracing that responsibility in this hearing today.

The Tension Between Privacy and National Security

The final report of the 9/11 Commission report does a masterful job of describing the horrendous terrorist attacks that took place on the morning of September 11, 2001, and of analyzing the factors that contributed to our nation's vulnerability to those attacks. The report goes on to make a number of thoughtful recommendations, including the urgent need that we use all of the information at our collective disposal to protect against further attacks, but that we do so only in ways that are consistent with protecting personal privacy.

---

[*] I gratefully acknowledge the assistance in the preparation of this statement of Fred H. Cate, a Distinguished Professor and director of the Indiana University Center for Applied Cybersecurity Research, who served as Reporter for the Technology and Privacy Advisory Committee.

The 9/11 Commission report does not suggest *how* we might exploit that information without invading privacy. The report identifies the goal, without providing any guidance as to the means. The Technology and Privacy Committee had spent the prior year addressing many of these issues about how we use information to protect national security without infringing on privacy.

Background of TAPAC

The history of TAPAC is fully laid out in our final report, the executive summary from which I attach to my prepared testimony, so I will only briefly recite it here. In early 2002, the Defense Advanced Research Projects Agency ("DARPA") announced that it was developing advanced information technologies which could access personally identifiable information in the fight against terrorism. The project—called "Terrorism Information Awareness" ("TIA")[*]—soon prompted serious public and congressional criticism centered on the possible use by government of personal information on U.S. citizens and permanent resident aliens.

To address these and other concerns, in February 2003 Secretary Rumsfeld appointed the Technology and Privacy Advisory Committee, the members of which were private citizens, independent from the government and "selected on the basis of their preeminence in the fields of constitutional law and public policy relating to communication and information management." *Establishment of the Technology and Privacy Advisory Committee*, 68 Fed. Reg. 11,384 (2003) (DOD, notice). He charged TAPAC with answering four questions:

1. Should the goal of developing technologies that may help identify terrorists before they act be pursued?
2. What safeguards should be developed to ensure that the application of this or any like technology developed within DOD is carried out in accordance with U.S. law and American values related to privacy?
3. Which public policy goals are implicated by TIA and what steps should be taken to ensure that TIA does not frustrate those goals?
4. How should the government ensure that the application of these technologies to global databases respects international and foreign domestic law and policy? U.S. Department of Defense, *Technology and Privacy Advisory Committee Charter* (2003).

In June 2004, TAPAC released its final report, containing its conclusions and 7 and 5 12 recommendations addressing data mining within the Department of Defense and throughout the federal government. Before turning to those conclusions and recommendations, I want to stress two features of the Committee and its work.

First, the panel was strictly bi-partisan, both in its membership and in the way it pursued its work. It was chaired by the Honorable Newton N. Minow, Senior Counsel to the law firm of Sidley Austin Brown & Wood, who served as chairman of the Federal Communications Commission under President Kennedy, and later served as chairman of the Carnegie Corporation,

[*] When first announced, the program was entitled "Total Information Awareness." The title was changed to "Terrorism Information Awareness" in May 2003.

Public Broadcasting Service, and The RAND Corporation, and vice chairman of the Commission on Presidential Debates. It would be hard to find a more impartial, skillful, or experienced public servant.

The other Committee members with whom I was privileged to serve were:

Floyd Abrams, a partner in the New York law firm of Cahill Gordon & Reindel, the William J. Brennan, Jr. Visiting Professor of First Amendment Law at the Columbia Graduate School of Journalism, and one of the nation's leading experts on the First Amendment.

Zoë Baird, President of the Markle Foundation, and previously was senior vice president and general counsel of Aetna, Inc., and an attorney in White House and in the Justice Department.

Griffin Bell, formerly Managing Partner of King & Spalding, a judge on the U.S. Court of Appeals for the Fifth Circuit, and Attorney General of the United States.

Gerhard Casper, President Emeritus of Stanford University and the Peter and Helen Bing Professor in Undergraduate Education at Stanford.

William T. Coleman, Jr., Senior Partner and the Senior Counselor in O'Melveny and Myers; he served as Secretary of Transportation during the Ford Administration.

Lloyd N. Cutler, founding partner of the law firm of Wilmer, Cutler & Pickering; he served as Counsel to Presidents Clinton and Carter.

The second feature is that Secretary Rumsfeld charged the Committee with considering not only laws applicable to privacy, but also "American values related to privacy." This important addition to the Committee's mandate obligated us to ask not only what the law concerning government use of personal information was, but what it *should* be.

The Prevalence of Government Data Mining and the Limits of Relevant Law

From the outset, the Committee was struck by two discoveries. The first was how widespread, not only in the Department of Defense, but throughout the federal government, data mining was. In fact, report by the General Accounting Office, released in May 2004 after the TAPAC finished its work, found 42 federal departments or agencies—including every cabinet-level agency that responded to the GAO's survey—engaged in (88), or were planning to engage in (34), 122 data mining efforts involving personal information. Thirty-six of those involve accessing data from the private sector; 46 involve sharing data among federal agencies. U.S. General Accounting Office, *Data Mining: Federal Efforts Cover a Wide Range of Uses* (GAO-04-548), May 2004, at 3, 27-64, tables 2-25.

The Committee's second discovery was how limited the federal law applicable to the government's use of personal information really was. The law that does exist is often too narrow

to ensure either that the government can access the data it really needs to protect national security and fight crime effectively or that individual privacy is protected in the process. In particular, that law depends significantly on whether the individual(s) involved are U.S. citizens, where the search takes place, whether the information has ever been disclosed to third parties, and the government's motivation for the search. In the face of new terrorist threats posed within the territory of the United States and global information technologies this system has grown increasingly unworkable.

So what the Committee found was widespread data mining, and little clarity in the law.

TAPAC's Recommendations

As a result, the Committee focused its deliberations, and ultimately its recommendations, on what the law should be to ensure that information is used to enhance national security without impinging on individual privacy or liberty. We unanimously agreed that the United States should use data mining to enhance national security; our recommendations then were focused on assuring that the privacy interests of U.S. persons are not compromised when it does so. Because those recommendations are included in the attached executive summary, I will not recite all of them here, but I would like to focus on six that are most relevant to today's hearing.

1. Privacy Tools

First, we thought it imperative that government data mining programs take advantage of the technological and other tools available to protect privacy. So, for example, we recommended requiring:

a. Data minimization—the least data consistent with the purpose of the data mining should be accessed, disseminated, and retained.
b. Data anonymization—whenever practicable data mining should be performed on databases from which information by which specific individuals can be commonly identified (e.g., name, address, telephone number, SSN, unique title, etc.) has been removed, encrypted, or otherwise obscured. Where it is not practicable to use anonymized data, or access to identifying information is required, the agency should comply with Recommendation 2.4 below.
c. Audit trail—data mining systems should be designed to create a permanent, tamper-resistant record of when data have been accessed and by whom.
d. Security and access—data mining systems should be secured against accidental or deliberate unauthorized access, use, alteration, or destruction, and access to such systems should be restricted to persons with a legitimate need and protected by appropriate access controls taking into account the sensitivity of the data.
e. Training—all persons engaged in developing or using data mining systems should be trained in their appropriate use and the laws and regulations applicable to their use. (Recommendation 2.2)

We also recommended special protection when data mining would involve the use of data from the private sector or other government agencies. (Recommendation 2.3)

2. Privacy Culture

Second, we thought it was critical that concern for privacy and other civil liberties be instilled at every level within agencies that engage in data mining. We therefore proposed that agency personnel receive appropriate training (Recommendation 2.2(e)), the creation of a policy-level privacy officer to help promote sensitivity to privacy throughout agencies (Recommendation 4), the appointment of external privacy advisors to help provide privacy-related input from outside of the agency (Recommendation 5), and that the agency head be charged specifically with creating "culture of sensitivity to, and knowledge about, privacy issues" throughout the agency (Recommendation 7).

3. Internal Accountability

Third, we believed that accountability was absolutely critical to protecting privacy, to ensuring that data mining was conducted efficiently and effectively, and to building public confidence in the government's data mining efforts. This objective undergirded many of our recommendations. We thought of accountability as occurring in two distinct settings: internal and external.

Internal accountability would be enhanced, we believed, first by ensuring that no agency engage in data mining involving personal information without making a conscious, thoughtful decision to do so, or without fully appreciating the potential privacy ramifications of its actions. So, for example, we recommended that data mining require written authorization by the agency head. (Recommendation 2.1) That written finding would demonstrate that a senior government official had thought through:

a. the purposes for which the system may be used;
b. the need for the data to accomplish that purpose;
c. the specific uses to which the data will be put;
d. that the data are appropriate for that use, taking into account the purpose(s) for which the data were collected, their age, and the conditions under which they have been stored and protected;
e. that other equally effective but less intrusive means of achieving the same purpose are either not practically available or are already being used;
f. the effect(s) on individuals identified through the data mining (e.g., they will be the subject of further investigation for which a warrant will be sought, they will be subject to additional scrutiny before being allowed to board an aircraft, etc.)
g. that the system has been demonstrated to his or her satisfaction to be effective and appropriate for that purpose;
h. that the system complies with the other requirements of this recommendation as enacted by law, executive order, or other means;
i. that the system yields a rate of false positives that is acceptable in view of the purpose of the search, the severity of the effect of being identified, and the likelihood of further investigation; and
j. that there is a system in place for dealing with false positives (e.g., reporting false positives to developers to improve the system, correcting incorrect information if

possible, remedying the effects of false positives as quickly as practicable, etc.), including identifying the frequency and effects of false positives. (Recommendation 2.1)

That written finding would also serve to ensure that a policy-level official (in almost every case an official whose appointment was subject to Senate confirmation), was involved in making the determination to go forward.

We believed internal accountability would also be fostered through the creation of a senior policy-level privacy officer (Recommendation 5), by regular audits of all data mining programs (Recommendation 2.5), by seeking the advice of external privacy experts (Recommendation 5), and through renewed efforts by the agency head to ensure the "effective operation of meaningful oversight mechanisms" (Recommendation 6).

4. External Accountability

Fourth, while accountability within an agency is essential, it is no substitute for external accountability, and it was here that our strongest—and most controversial—recommendations were focused. I suspect it is the failure to provide for meaningful external accountability that has contributed to public unrest about programs such as TIA and CAPPS II. Our goal was to help diffuse some of that controversy in the future by providing for meaningful external oversight.

TAPAC recognized that programs to enhance national security and public safety will often involve classified information or require speedy action, and so traditional accountability measures (such as public notice and opportunity to comment, or judicial review) may not work. Nevertheless, we believed that significant tools are available and should be required when the government accesses personal information about its citizens or legal aliens.

a. Judicial Review

One critical external accountability measure we recommended is recourse to the courts before conducting data mining with personally identifiable information about U.S. persons. (Recommendation 2.4) We recommended the Foreign Intelligence Surveillance Act court, to help provide for speedy and confidential review, but the particular court is not nearly as important as the concept of judicial review. The public understandably derives confidence from knowing that an independent, judicial authority is reviewing government data mining efforts. This is especially true when, because of secrecy concerns, the public may not have access to information about those efforts.

We stressed that judicial review could be obtained for specific searches or for entire data mining programs (Recommendation 2.4(a)(v)), and we provided that, in exigent circumstances, the review could be obtained after-the-fact (Recommendation 2.4(c)). Our goal in crafting these provisions was not merely to ensure that the process of judicial review not interfere with national security, but also to highlight that even the exigencies of the war on terrorism do not justify abandoning the vital principle of judicial review.

b. Congressional Oversight

The other essential component of external accountability is oversight by the Congress. You are the people's elected representatives and it is your unique duty to ensure that the people's business is carried out effectively, efficiently, and without compromising the people's rights. TAPAC therefore recommended that each agency's privacy officer have a direct reporting line to Congress, as you provided with regard to the Department of Homeland Security's privacy officer—a position ably filled by Ms. Nuala O'Connor Kelly, who appeared before TAPAC. We went a step further, however, to recommend that the agency head appear as well, and that the privacy officer and agency head jointly brief you, at least annually, on

a. the agency's compliance with applicable privacy laws;
b. the number and nature of data mining systems within the agency, the purposes for which they are used, and whether they are likely to contain individually identifiable information about U.S. persons;
c. the number and general scope of agency findings authorizing data mining;
d. the number and general scope of agency findings and court orders authorizing searches of individually identifiable information about U.S. persons; and
e. other efforts to protect privacy in the agency's collection and use of U.S. person data. (Recommendation 11)

These are serious obligations; we meant them to be. Nothing less guarantees you the information and regular access to senior personnel necessary to provide the accountability that the public expects.

To carry out these obligations, we made an equally bold recommendation that you take the steps necessary to streamline committee jurisdiction:

> To facilitate this reporting process and consistent, knowledgeable oversight, each house of Congress should identify a single committee to receive all of the agencies' reports. Other committees may have jurisdiction over specific agencies and therefore also receive reports from those agencies, but we believe it is important for a single committee in each house to maintain broad oversight over the full range of federal government data mining activities. To the extent the jurisdiction of congressional committees overlaps, we believe it is essential for Congress to clarify and clearly articulate the relative responsibilities of each committee, to avoid undermining either privacy protection or national security efforts. (Recommendation 11)

As a former Member of Congress, I am well aware of the uphill battle that such an effort involves, but we believed it is essential for meaningful oversight of both privacy and security.

5. Consistent Laws and Processes

Fifth, TAPAC recommended that all of the actions outlined above be carried out across the government. This would include adopting a single framework of legal, technological, training, and oversight mechanisms necessary to guarantee the privacy of U.S. persons in the context of national security and law enforcement activities; the appointment of a privacy officer in every federal agency; and the creation of an inter-agency coordinating committee and the use of external advisors to help ensure the consistent application of privacy laws and principles. (Recommendations 8-10)

TAPAC recognized that privacy protections would not necessarily be the same in every setting, but we believed it essential that they be consistent, based on common principles, and subject to uniform oversight.

The recent report of the 9/11 Commission only highlights the importance of these recommendations. It makes little sense to coordinate this nation's intelligence and national security activities, without going one step further to coordinate the laws and processes that ensure those activities respect our privacy and civil liberties.

6. Research

Finally, TAPAC recognized the importance of research into technological and other tools for making data mining more precise and accurate and for protecting privacy, as well as into the development of policies and laws to facilitate both data mining and privacy. (Recommendations 7, 12) One unfortunate consequence of Congress blocking further development of TIA was to prohibit further research by DARPA into both data mining and privacy.

This is regrettable; our nation desperately needs to understand better the technological, behavioral, and policy tools for using information effectively and appropriately, whether to fight terrorism, apprehend criminals, or otherwise serve the public. There are many private initiatives to expand our understanding—my own program at the George Mason School of Law is one example—but if we are serious about using information to fight terrorism and serious about protecting privacy while doing so, it is going to require the investment of public funds.

The Link Between Privacy and National Security

I began by describing the tension between privacy and national security; I would now like to highlight what TAPAC saw as the essential link between the two. Many of our recommendations that may have been motivated by a desire to protect privacy, also contribute to enhancing security as well. Data minimization, for example, is a key privacy tool, but it also helps protect intelligence agencies from being overwhelmed by irrelevant data. Tools for data correction are another example: data mining with inaccurate data certainly threatens privacy and civil liberties, but it also threatens security as well. Any system of data analysis that is not concerned with data quality and accuracy is likely to compromise both privacy and security.

Privacy and national security are also inherently linked because American values will not accept the latter at the cost of the former. Recent protests over TIA, CAPPS II, and other programs have shown that the American public will not either. Inadequate, unclear, or uncertain privacy laws are slowing the development of new and promising data mining programs, they are undermining research into this important weapon in the war on terrorism, and they are hampering the very data sharing that the 9/11 Commission wisely recommended. Clearing up this mess is critical *both* to protecting our privacy *and* to protecting our security.

The Role of the Judiciary Committee

TAPAC took no position on which committee in Congress should take the lead on this vital effort, but I believe the Committee on the Judiciary is an ideal choice. The issues involve come within the jurisdiction of many committees—Armed Services, Intelligence, Commerce, Ways and Means, and others—but the foundational issue that cuts across all of these different settings is the constitutional and legal framework applicable to data mining. That is the fundamental question—the starting place for all other analysis. That is your turf. And I assume that is why you have called these important hearings today.

Conclusion

Throughout Washington, throughout the nation, citizens are lining up to be searched before entering federal buildings or boarding aircraft. The mail is delayed so it can be scanned. Luggage is x-rayed and rummaged through. Roads are closed, entrances blocked with concrete barricades, access to public resources denied. Surveillance cameras and identity checks are replacing anonymity. The result is not just inconvenience or annoyance, it is a vast toll on our economy and productivity and a profound intrusion on our privacy and most basic civil liberties.

Think of the effect on government. The threat of terrorism has turned the People's House into an armed citadel. The Capitol, the very heart of democratic government, is under siege, and with it our privacy, liberty, and most cherished values.

Data mining—as both the 9/11 Commission and TAPAC noted—is a vital weapon in the war on terrorism. It poses grave risks to privacy, but there are numerous steps, many (but certainly not all) of which are outlined in the TAPAC report, that can reduce or eliminate those risks. Those steps may not only protect privacy, but also enhance security as well. More importantly, when pursued effectively and subject to appropriate safeguards, data mining may threaten privacy and civil liberties far less than the other tools on which we rely so heavily and so regrettably today.

Thank you.

Attachment